U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

July 12, 2005

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for forwarding questions for the record from Members of the Committee, in your letter dated May 19, 2005. Enclosed are the answers to question 1-19 and 24-44, which include all questions related to the USA PATRIOT Act. The remaining questions, which are unrelated to the USA PATRIOT Act, will be sent to the Committee shortly.

We hope that this information is helpful to you as you consider reauthorization of the USA PATRIOT Act. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable John Conyers, Jr.
Ranking Minority Member

House Judiciary Committee Minority Questions for the Record

1) **On numerous occasions in the past, I and other Democratic members have submitted questions to the Department concerning the USA PATRIOT Act and other terror-related issues. Attached are a number of such letters that have been ignored. Could you please appraise us whether a response is pending, and if not, why not. As a general matter, please explain the rule or standard for responding to Minority initiated questions.**

ANSWER: There were no attachments to your questions for the record so we are unable to fully respond. However, the Department has conducted its own review of outstanding congressional correspondence from Democratic Members and do not believe there exist "a number of [USA PATRIOT Act] letters that have been ignored." In fact, according to our records, there are no outstanding letters from any Democratic Members of the House Judiciary Committee related to the USA PATRIOT Act.

2) **At the hearing, you expressed a willingness to open up the files on the Brandon Mayfield investigation, subject to a purported limitation imposed by the ongoing litigation of the matter. You stated,**

"Again, Congressman, this matter is in litigation so I'm likely to be limited about what information I can share with you, but I'm happy to go back and see what we can do to provide information to the committee in connection with this case." See Transcript, "Oversight Hearing on the USA Patriot Act: A Review for the Purpose of Reauthorization," at 27:557-561 (April 6, 2005).

We reviewed numerous precedents and found that the presence of ongoing litigation is not a barrier to the broad and encompassing power in Congress to obtain information. This power reaches all sources of information in open and closed cases, subject only to narrow privilege exceptions. See Sinclair v. United States, 279 U.S. 263 (1929) (rejecting in unequivocal terms the witness' contention that the pendency of lawsuits provided an excuse for withholding information); see also McGrain v. Daugherty, 272 U.S. 135 (1927); Eastland v. United States Servicemen's Fund, 421 U.S. 491 (1975); Watkins v. United States, 354 U.S. 178 (1957). In light of these precedents, we reiterate our request for all records in the Brandon Mayfield investigation relating to the following:

A. Any Foreign Intelligence Surveillance Act ("FISA") orders issued in the investigation, approving the physical search or electronic surveillance conducted on Mr. Mayfield, his office, his home or any other property;
B. Any Prosecutorial memoranda detailing deliberations on the investigation;
C. All audiotape recordings, telephone wiretaps, telephone records the FBI obtained from Mr. Mayfield's home or office, other audio interceptions or transcripts;

D. Any documents seized in evidence.

If you are asserting privilege with regard t any of this information, please substantiate the privilege.

ANSWER: After reviewing the transcript, we have confirmed that at the hearing, the Attorney General did not agree to "open up the files" relating to this matter. The Attorney General agreed, after acknowledging that this matter is in litigation, to "see what we can do to provide information to the Committee in connection with this case." The Department has provided additional information on this matter by supplying to the Committee a copy of a letter, dated April 26, 2005, to Senator Feinstein, which we have attached for your convenience. This matter remains in active litigation and under internal investigation, and so we are limited in our ability to provide additional information.

3) **Please articulate the standard you suggest this Committee use when deciding whether to reauthorize particular sections of the PATRIOT Act? It appears from numerous public statements that your department sees the infrequent use of a provision as good restraint, and the exorbitant use of other provisions as a sign of their usefulness.**

ANSWER: When deciding whether to reauthorize those provisions of the USA PATRIOT Act scheduled to sunset at the end of this year, the Committee should consider whether a particular section has helped achieve the objectives we share: safeguarding the security of the American people while preserving our civil liberties. In addition, the Department uses the tools provided by the USA PATRIOT Act as appropriate. Some provisions therefore will obviously be used more frequently than others. In determining whether to reauthorize the vital tools included in the USA PATRIOT Act, the Committee should also consider that it has been confirmed repeatedly at recent oversight hearings that there have been no substantiated abuses of the USA PATRIOT Act. Moreover, the Department's Office of the Inspector General to date has not documented in the semiannual reports mandated by section 1001 of the USA PATRIOT Act any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the Act.

4) **You confirmed that your department has used Section 215 of the PATRIOT Act 35 times. What type(s) of information was sought? What type of entity was the recipient of the request?**

ANSWER: As the Attorney General indicated at the hearing, as of March 30, 2005, information sought under the authority provided for by section 215 included driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices. Also through March 30, 2005, no section 215 orders were sought to obtain library or bookstore records, medical records, or gun sale records.

5) **In how many investigations has information obtained from FISA orders been**

used for investigations of "federal crimes of terrorism," as that term is defined in 18 U.S.C. § 2332b(g)(5)? What federal crimes of terrorism were being investigated?

ANSWER: The Department does not systematically or routinely track how information obtained pursuant to the Foreign Intelligence Surveillance Act is used in investigations of "federal crimes of terrorism" as defined in the Committee's question.

6) **In how many investigations has information obtained from FISA orders been used for investigations of criminal offenses other than "federal crimes of terrorism," as that term is defined in 18 U.S.C. § 2332b(g)(5)? What such offenses were being investigated?**

ANSWER: The Department does not systematically track how information obtained pursuant to the Foreign Intelligence Surveillance Act is used in connection with investigations of crimes other than "federal crimes of terrorism" as defined in the Committee's question.

7) **Pursuant to section 223 of the PATRIOT Act (civil liability), have any claims been filed against the United States or has any official of the Department of Justice been sued or disciplined? What was the nature and outcome of such claim(s)?**

ANSWER: The Department is aware of no administrative or federal court claims filed citing section 223 of the USA PATRIOT Act (18 U.S.C. § 2712).

8) **How many single-jurisdiction search warrants have been issued pursuant to Rule 41(a)(3) of the Federal Rules of Criminal Procedure as amended by section 219 of the PATRIOT Act?**

ANSWER: The Department does not systematically track how many single-jurisdiction search warrants have been issued pursuant to Rule 41(a)(3) of the Federal Rules of Criminal Procedure. While we do not track the number, we can tell you that the Department has used section 219 in several investigations, including an investigation that led to the prosecution of several individuals for acting as unregistered agents of the Iraqi intelligence service in 2003, before and during our military action in Iraq. The U.S. Attorney's Office for the Southern District of New York obtained a search warrant from a magistrate judge in New York authorizing the search of the premises of a suspect in Maryland who was to be arrested in conjunction with the execution of the search warrant. The suspect was charged with, among other things, participating in illegal financial transactions with a state sponsor of terrorism, specifically Iraq. Prosecutors report that the ability to use section 219 was crucial in coordinating the successful multi-district plan of arresting one of the defendants and conducting the search simultaneously. Because of the high-profile nature of the particular defendant, section 219 was also critical to the Department's ability to limit the number of people who had knowledge of the operation prior to its execution, which helped to assure its success.

9) **How many times has the Department of Justice disclosed grand jury information pursuant to its power under section 203 of the PATRIOT Act? Has this section ever been used to obtain, and then disclose, entire databases of data to the government? If so, what types of databases were obtained and to whom were they given?**

ANSWER: We are in the process of compiling data responsive to your question as to how many times the Department has disclosed grand jury information under section 203(a). With respect to whether this section has ever been used to obtain and then disclose entire databases to the Government, let me clarify that section 203 is not used specifically to obtain information for disclosure to the intelligence community, as the question seems to imply. The material disclosed under section 203(a) is material obtained in the course of an existing criminal investigation which involves foreign intelligence and counterintelligence information. If prosecutors obtain such information in the course of their grand jury investigation, they are obliged by section 203(a), section 905 and related Attorney General Guidelines to share this information in order for the intelligence community to better "connect the dots." When notified about such disclosures, we do not receive information about the nature of the material disclosed. Therefore, we do not know whether any of these disclosures involve databases.

10) **You have confirmed that the Department has attained 155 "sneak and peek" searches under Section 213 of the PATRIOT Act. How many of those 155 cases were terror related? How many prosecutions have resulted, at least in part, from sneak and peek searches? And how many of those prosecutions were terror related?**

ANSWER: Since reporting the figures cited in this question, we have discovered that, in our past surveys of section 213 usage, some U.S. Attorneys' Offices had mistakenly reported extensions of delayed-notice search warrants as new warrants or had reported the same warrant in multiple surveys. These errors caused the numbers that we previously reported to Congress to overstate our use of section 213. To the best of our knowledge, the number of uses of delayed-notice search warrants issued from the enactment of the USA PATRIOT Act through January 31, 2005, is 153. At least eighteen of these warrants involved terrorism-related offenses or terrorism-related suspects. This data was collected in surveys that were sent to every United States Attorney's Office. However, the survey did not include any inquiries relating to the prosecutions resulting from these investigations. As a result, we can report that hundreds of convictions have taken place in investigations where delayed-notice search warrants have been used, but we do not have the data to quantify the number of prosecutions precisely.

11) **How many emergency FISA orders has the Attorney General authorized since September 11, 2001?**

ANSWER: This classified number is reported as part of the Attorney General's Semi-Annual Report (SAR) to Congress on use of FISA. It is our understanding that these reports are available for review by any Member and by appropriately cleared staff with a need to know through the Intelligence Committee that receives them. For your convenience, however, we have

provided it in the attached classified annex.

12) Has the DOJ offered any classified evidence in immigration proceedings that have been instituted since March 1, 2003?

ANSWER: In removal proceedings, the Department of Justice is the adjudicator, not the prosecutor. Accordingly, the Department does not offer evidence in those proceedings. The Department of Homeland Security (DHS) represents the United States Government in removal proceedings and would offer any such evidence. Our records do not reflect that DHS has offered classified evidence in any proceedings that were initiated after March 1, 2003.

13) How many protective orders have been requested under 8 C.F.R. § 1003.46? How many of those were granted?

ANSWER: To date, 26 Motions for Protective Orders have been filed. Of those, 23 were granted, 1 was denied, and 2 are pending.

14) You confirmed that you had received information from libraries, but not through Section 215. Please provide unclassified information on the number of times Section 505 of the USA PATRIOT Act have been used in libraries. What other authorities have been used to request or accept information from libraries in terror-related cases?

ANSWER: Information regarding National Security Letters (NSLs), including the number of requests made pursuant to these authorities, is classified. However, as required by statute, the use of NSL authorities is subject to extensive reporting requirements to and oversight by several committees of Congress. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence receive reporting under 18 U.S.C. § 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act. The Senate Banking, Housing, and Urban Affairs Committee and the House Financial Services Committee receive reporting under the Fair Credit Reporting Act. The Senate and House Judiciary Committees receive reporting under 18 U.S.C. § 2709. The Department transmitted these reports to the respective Committees on December 16, 2003; June 29, 2004; and most recently on April 28, 2005. Therefore, Congress currently has all information that is required under the relevant statutes. We acknowledge that certain reports were not filed within the exact statutory time frame and efforts are underway to ensure continued accurate and timely filing. It is our understanding that these reports are available for review by any Member and by appropriately cleared staff with a need to know through the Committees that receive them.

As a matter of law, libraries could and have provided information or documents voluntarily to the FBI; could and have provided information or documents in response to grand jury subpoenas; or could provide information or documents in response to an order issued by the FISA Court pursuant to section 215 of the USA PATRIOT Act. However, the Attorney General declassified the fact that none of the section 215 orders has been issued to libraries as of March 30, 2005.

Additional classified information responsive to this question is supplied under separate cover.

15) **For the past 20 years, the government has issued the total number of FISA applications, the number granted and the number denied without harm to our national security. Why then won't the Justice Department issue an unclassified number of orders under Section 215 of the Patriot Act, which should have fewer national security implications? Aren't there other FISA numbers that could be released to the public without harming national security? What about the number of Section 215 orders, and the number of National Security Letters?**

ANSWER: The Attorney General declassified the number of section 215 orders as of March 30, 2005. As of that date, there had been thirty-five such orders.

The Department of Justice, in consultation with the Intelligence Community, analyzes FISA-related statistics that can be released to the public without harming national security. At this time, it is the Department's judgment that release of any further FISA-related statistical information could pose an unacceptable risk to national security. However, the Department does make extensive reports to Congress in the Semi-Annual Report (SAR) to Congress on the use of FISA. It is our understanding that these reports are available for review by any Member and by appropriately cleared staff with a need to know through the Intelligence Committee.

16) **The government often seems to blur the distinction between criminal investigations, which carry certain protections, and national security investigations, which are broader and more secretive. For example, with regard to Section 215 of the Patriot Act, the Justice Department claims that it just wanted to give prosecutors the same tools for going after terrorists that they have for going after other criminals (such as the Mafia, or ordinary street crime). If supporters of the Patriot Act are going to argue that changes to the law are needed to give the government the same powers in foreign intelligence investigations that it already had in criminal investigations shouldn't the same safeguards apply as well?**

ANSWER: As a general matter, tools that are available in criminal investigations should be available in national security investigations--in other words, it should not be more difficult to investigate terrorism cases than drug cases. Given the basic differences between national security investigations, which may not end in criminal prosecution, and criminal investigations, however, it is not the case that the shape of these tools should be exactly the same in the two situations. This is particularly true in view of the inherently sensitive nature of national security investigations, which can often span significant periods of time.

Turning to section 215, however, that provision specifically is *more* protective of civil liberties than a similar tool used in criminal investigations, the grand jury subpoena. A federal

judge or magistrate must authorize a section 215 order, whereas a grand jury subpoena issues without prior court review or authorization. Section 215 is also narrower in scope than a grand jury subpoena; it can be used only (1) "to obtain foreign intelligence information not concerning a United States person" or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes or even domestic terrorism, whereas a grand jury can obtain business records in investigations of *any* federal crime. In addition, section 215 expressly protects First Amendment rights, providing that an investigation of a United States person may not be done solely on the basis of First Amendment activity. Finally, the use of section 215 is subject to congressional oversight; every six months, the Attorney General must "fully inform" Congress on how that provision has been implemented.

17) **The SAFE Act changes Section 213 (which authorizes delaying notice of search warrants in certain cases) to state that instead of an open-ended delay, the Justice Department can receive an initial 7-day delay before notifying someone of a search warrant, in certain circumstances. DOJ has challenged this as an unreasonable requirement. But, isn't it the case that 7-days was the general length of delay authorized by courts before the Patriot Act?**

ANSWER: Numerous courts concluded that delayed notice search warrants were permissible under the Fourth Amendment before the enactment of the USA PATRIOT Act, but there was no concerted tracking of the length of delays that were authorized. (Indeed, many of these decisions went unpublished.) It is therefore not possible to determine the "general" length of delay previously authorized by the courts.

The Fourth Circuit's conclusion in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2002), that a delay of 45 days would not violate the Fourth Amendment would tend to undermine any notion that seven days was a standard period. To be sure, the Ninth Circuit did hold that seven days would be appropriate absent some additional showing in *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986), but both of these courts came to their respective conclusions based on a reasonableness inquiry pursuant to the text of the Fourth Amendment. With section 213, Congress codified that reasonableness inquiry, allowing judges familiar with the facts of particular investigations to determine what length of delay is appropriate. The Department supports the language of section 213; although there may be circumstances where seven days is an appropriate delay, the Department could not support imposing a hard and fast rule to that effect.

18) **Section 206 of the Patriot Act creates "roving wiretaps" in intelligence cases (i.e., outside of the normal Title 3 criminal wiretaps), which allows the government to get a single order that follows the target from phone to phone. In addition, the Intelligence Authorization bill passed shortly after the Patriot Act allows the government to issue "John Doe" wiretaps, where the phone or facility is known, but the target is not known. The way that the two laws were written seems to allow for a general wiretap - one that follows an unknown suspect from unknown phone to unknown phone. Your Department claims that this authority is available in standard criminal cases.**

Please list the jurisdictions that allow you to install a wiretap after neither designating the target nor a specific phone.

ANSWER: Section 206 of the USA PATRIOT Act provided national security investigators with the authority to conduct court-approved multi-point (sometimes called "roving") surveillance of foreign powers or agents of foreign powers, such as terrorists or spies, who may take steps to thwart surveillance. Multi-point wiretap authority has been available in criminal investigations since 1986, and section 206 simply added this authority to FISA.

The premise of the question, that "general wiretaps" that follow "an unknown suspect from unknown phone to unknown phone" are now permissible, is simply incorrect. When applying to the FISA Court for a surveillance order, the Government must provide the court with the target's identity if known, or otherwise a description of the target. This ability to provide a description could be critical in cases where the Government knows a great deal about a target but does not know his identity because, for example, he is a spy trained to conceal it. And the possibility of providing a description does not reduce the safeguards placed on section 206's "roving" wiretap authority. Every "roving" surveillance order is tied to a particular target. The court order authorizing surveillance then allows surveillance of the target to continue if he switches phones; it does not allow the Government to switch surveillance to a different target. Moreover, to authorize surveillance ("roving" or not) the FISA Court must find probable cause that the target of the surveillance is a foreign power or an agent of a foreign power. Thus, in cases where the Department does not know the identity of the target, the Department is required to present a sufficiently particular description of a target to allow the FISA Court to make the determination that the specified target is a foreign power or an agent of a foreign power. And the FISA Court may authorize "roving" surveillance only where it finds that the target's actions, such as a pattern of frequently changing cell phones, may thwart surveillance.

19) **Section 218 has been described as tearing down the "wall" between intelligence and criminal investigations, and the Department has been adamant that it should not sunset. However, the PATRIOT Act has already created permanent authorization for information sharing between the criminal and intelligence agencies: Section 905 requires the Attorney General to provide terror related information to the Director of National intelligence that is uncovered in the process of a criminal investigation, and section 504 allows FISA information to be given to the criminal division. Don't these two sections ensure that real terror and intelligence information can be shared? Doesn't Section 218 only facilitate criminal prosecution against those who are not guilty of terror-related offenses?**

ANSWER: Section 218 was instrumental in eliminating both perceived statutory and cultural barriers to information sharing that had developed over time, and the Department strongly supports reauthorizing that provision. As witness after witness has recently testified, our culture of enhanced information sharing has been critical to our efforts in combating terrorism and securing the values we cherish. Section 504 provides that coordination between intelligence agents and law enforcement officers shall not preclude the certification required for FISA, but

section 218 remains necessary to make clear what the actual standard for such certification is. Allowing section 218 to sunset would therefore risk significantly impeding intelligence sharing efforts.

For your convenience, we have also attached our letter to Congressman Scott which details this issue further.

20) Does any department or agency of the U.S. government have the legal authority to transport U.S. citizens or non-citizens to foreign governments that practice torture or other inhumane treatment? Please provide an unclassified and classified copy of any document(s) pertaining to such authority.

ANSWER: The response to this question will be provided separately.

21) Does any department or agency of the U.S. government have the legal authority to transport foreign nationals to foreign governments for the purpose of obtaining information? Please provide an unclassified and classified copy of any document(s) pertaining to such authority.

ANSWER: The response to this question will be provided separately.

22) Has the Justice Department prosecuted American personnel who transported U.S. citizens or non-citizens to foreign governments that practice torture or other inhumane treatment? If not, why?

ANSWER: The response to this question will be provided separately.

23) (a) What categories of persons currently in U.S. military custody are excluded from the protections of the U.N. Convention Against Torture?

ANSWER: The response to this question will be provided separately.

(b) What categories of persons currently in U.S. military custody are excluded from the protections of the Geneva Conventions?

ANSWER: The response to this question will be provided separately.

24) How many individuals has the Department detained in the war on terror? Of those how many are known to have a connection to the 9/11 attacks or Al Qaeda? How many have no known connection to the 9/11 attacks or Al Qaeda? Please list the authorities for detaining both groups.

ANSWER: Without further parameters, it is difficult to answer your question. As you are aware, there are many reasons that individuals may be detained by the Department – among

other reasons, they may be arrested and ordered detained pre-trial by a court; they may be detained after they are convicted and sentenced; they may be detained pursuant to material witness warrants; or they may be detained administratively for immigration proceedings. Once detained, individuals may be released in some circumstances by a court on bond or other conditions.

To date, since September 11, 2001, we have charged over 400 defendants in matters arising from terrorism investigations with an international nexus. The Department does not differentiate among those cases that specifically involve al Qaeda, because the connections defendants have to al Qaeda vary significantly – from full-fledged operatives such as shoe-bomber Richard Reid, to those who have been known to funnel money to al Qaeda, to those seeking to join or fight alongside the terrorist organization, like the Portland Cell defendants. Sometimes, a defendant's al Qaeda connections are not completely known, or they may be classified and not part of the public record. However, it is public that a number of individuals have been charged with and convicted of crimes that connect them to al Qaeda. Some examples, though not an exhaustive list, include:

- Zacarias Moussaoui, who recently pleaded guilty to a number of crimes, including providing material support to a terrorist organization (18 U.S.C. § 2339B).
- John Walker Lindh, who pleaded guilty to providing material support to a terrorist organization (50 U.S.C. § 1705(b)).
- Iyman Faris, who pleaded guilty to providing material support to a terrorist organization (18 U.S.C. § 2339B).
- Shoe-bomber Richard Reid, who pleaded guilty to a number of charges, including placing a destructive device aboard an aircraft (49 U.S.C. § 46505) and attempted use of a weapon of mass destruction (18 U.S.C. § 2332a).
- Saajid Badat, charged in the District of Massachusetts with a number of charges related to his conspiracy with Richard Reid (18 U.S.C. §§ 32, 2332A, 2332, 1113, 924; 49 U.S.C. §§ 46505, 46506).
- Uzair Paracha, currently charged in the Southern District of New York with providing material support to al Qaeda (18 U.S.C. § 2339B).
- Ahmed Abu Ali, charged in the Eastern District of Virginia with several crimes, including providing material support to al Qaeda (18 U.S.C. § 2339B) and providing material support to terrorists (18 U.S.C. § 2339A).
- Umar and Hamid Hayat, recently charged in the Central District of California with making false statements relating to their participation at an al Qaeda training camp (18 U.S.C. § 1001).

To be clear, the above data reflects cases identified by the Criminal Division as matters arising from terrorism investigations with an international nexus. These cases include certain investigations conducted by Joint Terrorism Task Force (JTTF) agents and any other cases known to the Criminal Division in which there is evidence that an individual was engaged in terrorist activity or associated with terrorists or foreign terrorist organizations. The charges and convictions tracked by the Criminal Division reflect not only terrorism charges such as violations of the material support statutes, 18 U.S.C. §§ 2339A and 2339B, but also non-terrorism charges

such as immigration, firearms, and document fraud violations that have some nexus to international terrorism. It should be noted, however, that the Criminal Division tracks a subset of cases that are reported through the United States Attorneys' Offices (USAOs) case management system. The USAO's case management system reflects that, during Fiscal Year 2004, U.S. Attorneys' Offices filed a total of 570 terrorism and anti-terrorism cases against 725 defendants. For the purposes of this system, "Terrorism" cases include International Terrorism, Domestic Terrorism, Terrorist Financing, and Terrorism-Related Hoaxes, and "Anti-Terrorism" cases include immigration, identity theft, OCDETF, Environmental, and Violent Crime - all in cases where the defendant is reasonably linked to terrorist activity or where the case results from activity intended to prevent or disrupt potential or actual terrorist threats.

25) **Will you support the extension of the assault weapons ban so that terrorists in the United States cannot obtain such harmful weapons and cause mass casualties on American city streets?**

ANSWER: While not related to the USA PATRIOT Act, the Attorney General has indicated he supports the President's position on this matter. And the President has made clear that he stands ready to sign a reauthorization of the Federal assault weapons ban if it is sent to him by Congress. The Department of Justice is committed to vigorous enforcement of Federal firearms laws and will enforce any law Congress may enact extending the now-expired assault weapons ban.

26) **Considering how the FBI mishandled the Madrid bombing investigation and detained an innocent person, has the Department reviewed the alleged evidence against other detainees and material witnesses to see if that evidence was valid? If not, why not?**

ANSWER: Department prosecutors are well aware of their continuing obligation to review evidence and assess the strength of the cases they are prosecuting. The Department's policy, as stated in the Principles of Federal Prosecution and the United States Attorneys' Manual, is that a prosecutor should not bring charges against an individual unless the prosecutor can reasonably expect to prove those charges beyond a reasonable doubt by legally sufficient evidence at trial. The attorney for the Government should commence or recommend Federal prosecution of a person only if that attorney believes that the person's conduct constitutes a Federal offense and that the admissible evidence will probably be sufficient to obtain and sustain a conviction. No prosecution should be initiated against any person unless the Government believes that the person probably will be found guilty by an unbiased trier of fact. Department prosecutors are also well aware of their ongoing obligations under the Supreme Court's decision in *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny, which oblige prosecutors to turn over to the defense material evidence that is favorable to the defendant. This evidentiary review and assessment takes place throughout the preparation of a case. If at any time, the prosecutor concludes that there is not sufficient evidence to show that the defendant committed a charged offense, or concludes that the defendant did not commit a charged offense, it would be expected that the prosecutor would seek leave from the court to dismiss that charge.

Individuals may also be detained as material witnesses, in which case they are entitled to the protection afforded by the federal material witness statute. 18 U.S.C. § 3144. These protections include a judicial hearing and the right to counsel. They are detained so that their testimony can be obtained and are released from custody once that testimony is secured. As we discuss in response to question 40, sometimes such witnesses do not testify before a grand jury. This may occur for a variety of case-specific reasons, including that their testimony is taken by way of deposition and then they are released, or their expected testimony is determined to be cumulative of other witnesses and is no longer needed, or they arrive at an understanding with the prosecution to cooperate in the investigation.

27) **Assume that a stored recording of a telephone conversation is made by a network administrator without notice to the two parties. Do the two parties to the telephone conversation retain the same "reasonable expectation of privacy" in the stored conversation that they would have if the conversation was not stored? If so, would the Fourth Amendment protections be lower in any respect than those set forth in Berger v. New York?**

ANSWER: In general, a network administrator could not legally make and store such a recording without the consent of a party, unless the interception were made either a) to protect the rights and property of the network's owner or b) as a necessary part of providing the communication service. *See* 18 U.S.C. §§ 2511(1)(a) (general prohibition on interception of wire communications), 2511(2)(a)(i) (exception for protection of provider and provision of service). Based on the information provided, we do not believe that warehousing subscriber conversations would qualify as a necessary activity incident to providing telephone service.

Although private searches (including wiretapping) undertaken without Government involvement do not implicate the Fourth Amendment, and thus would not trigger constitutional suppression, 18 U.S.C. § 2515 provides a statutory suppression remedy prohibiting the fruits of illegal non-governmental eavesdropping, or evidence derived therefrom, from being introduced as evidence in any proceeding.

28) **Does your answer to Question 27 differ if the network administrator has provided general notice, such as through the terms of use, that caching and other storage of telephone conversations may occur for network security and other reasons?**

ANSWER: User consent, including that effectuated through terms of service, may serve as the basis for lawful authorization to monitor otherwise private communications. *See* 18 U.S.C. § 2511(2)(d) (consent of a party to the communication); *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998). In this respect, the Wiretap Act mirrors the consent exception to the Fourth Amendment. In each case, the scope of consent turns upon the particular facts and circumstances of the waiver.

29) **Assume that one party to a telephone conversation, which is conducted by VoIP on a computer, keeps a stored record of the conversation on that**

computer. Assume that the other party does not know the conversation is being recorded. Does either party to the conversation have a "reasonable expectation of privacy" in the contents of that conversation, so that Fourth Amendment protections apply?

ANSWER: Although both parties may have a reasonable expectation that their private conversation will not be intruded upon by others, neither party has a reasonable expectation of privacy with respect to the other participant. *See Hoffa v. United States*, 385 U.S. 293, 301-03 (1966) (articulating doctrine of "misplaced confidence"). It is settled law that an unwitting party has no Fourth Amendment right of privacy in a recording made by the other party to a communication. *See, e.g., United States v. Felton*, 753 F.2d 256, 259 (3rd Cir. 1985) ("we cannot see how the expectation of privacy arises when the recording of a conversation is made by [one's] own confederate").

The maker of the recording may or may not have an expectation of privacy in the recording, depending on where it is maintained. A tape kept in one's house would be subject to the same Fourth Amendment protections as other personal effects; by contrast, a digital recording left on a computer owned and used by others – such as a shared terminal in an office reception area – might enjoy no such protection, depending on the specific circumstances.

30) **Does your answer to Question 29 differ if both parties know the conversation is being recorded? Has the party who is not doing the recording thereby consented to waiving Fourth Amendment protections?**

ANSWER: As explained in response to Question 29, the consent of one party is sufficient for Fourth Amendment purposes.

31) **Does Section 209 as it currently exists allow law enforcement seizure of stored wire communications other than voice mails?**

ANSWER: By its terms, section 209 authorizes law enforcement to compel the production of any stored "wire communication."

32) **Does Section 209 as it currently exists apply to the fact setting of Question 27?**

ANSWER: It is arguable that section 209 does not apply to the facts of Question 27, as an illegally made recording of a conversation is arguably neither in "electronic storage" (as defined at 18 U.S.C. § 2510(17)) nor within the scope of 18 U.S.C. § 2703(b)(2), and thus not governed by subsections 2703(a) and (b) of Title 18, respectively.

33) **Does Section 209 as it currently exists apply to the fact setting of Question 28?**

ANSWER: Yes.

34) **Does Section 209 as it currently exists apply to the fact setting of Question 29?**

ANSWER: No. By its terms, section 209 applies only to the acquisition of stored wire communications from a service provider.

35) **Does Section 209 as it currently exists apply to the fact setting of Question 30?**

ANSWER: No. By its terms, section 209 applies only to the acquisition of stored wire communications from a service provider.

36) **Assume that VoIP telephone transmissions are done through a "store and forward" system in which there is transient storage of phone conversations as packets move from one part of the Internet to the next. Would this form of storage be enough to permit seizure of the stored recordings of telephone conversations under Section 209? Would it be enough under the panel decision in U.S. v. Councilman? Would it be enough under the Department of Justice position as set forth in the briefs in U.S. v. Councilman for the en banc First Circuit?**

ANSWER: The Department believes that such ephemeral storage is not subject to section 209, which may not be used to conduct prospective (i.e., ongoing and continuous) collection of communications content functionally equivalent to a wiretap. A recent decision of the United States Court of Appeals for the First Circuit – *United States v. Councilman*, 373 F.3d 197, *vacated and withdrawn*, 385 F.3d 793 (2004) – adopted a narrow interpretation of the term "interception" precluding its application to stored communications; taken to its logical conclusion, this holding would in theory imply that section 209 could be used to acquire transiently stored communications on an ongoing basis. Asserting in its memoranda of law the view that this decision is fundamentally incorrect, the Department sought and obtained *en banc* review. The panel decision, as noted above, has been vacated, and the full Court of Appeals has the case under consideration.

37) **Under Section 209 as it currently exists, are there any circumstances in which law enforcement can seize stored voice mail or a stored telephone conversation recording by use of a 2703(d) order or any other procedure that is less strict than a search warrant issued by a neutral magistrate?**

ANSWER: Section 2703(a) of Title 18, United States Code, states that stored wire communications in "electronic storage" – that is, not yet retrieved from the service provider by the user – for more than 180 days may be obtained under the authority of section 2703(b). The latter provision permits such communications, as well as those no longer in "electronic storage" (such as messages accessed by the subscriber and left thereafter on the provider's system), to be obtained by three separate means:

- warrant
- a grand jury, trial, or administrative subpoena, with prior notice to the customer
- an "articulable facts" court order under § 2703(d), with prior notice to the customer

See § 2703(b)(1)(B).

38) Please provide the Committee with information on the extent to which the new authority in Section 209 has been used in anti-terrorism cases. Has the new authority been used in any anti-terrorism investigations or prosecutions? Approximately what proportion of uses of the new authority has been for use in anti-terrorism cases?

ANSWER: Section 209 of the USA PATRIOT Act allows law enforcement to obtain voice mail stored with a third party provider by using a search warrant, rather than a wiretap order. The Department does not maintain a comprehensive record of all such search warrant requests and therefore we cannot provide the exact number of section 209 warrants that have been issued in anti-terrorism cases or the proportion of section 209 warrants that have been terrorism-related. However, we can confirm that since passage of the Act, such warrants have been used in a variety of criminal cases to obtain key evidence, including voice mail messages left for foreign and domestic terrorists.

39) How many FISA searches have been conducted under the standard set out in section 218 of the PATRIOT Act? How many prosecutions for terrorism-related crimes have been initiated as a result of such a search? How many prosecutions for non-terrorism related crimes have been initiated as a result of such a search? How many convictions have been obtained?

ANSWER: The response to this inquiry is classified and is, therefore, provided in the classified annex.

40) Since 9/11, how many times has the Department used its authority to detain material witnesses under 18 U.S.C. section 3144? How many of these individuals actually ended up testifying before a grand jury?

ANSWER: As you know, material witness warrants are generally issued in conjunction with a grand jury investigation, and while the Department is committed to keeping Congress informed about the issue of material witness warrants, we must also respect the letter and spirit of the grand jury secrecy rules, Fed. R. Crim. P. 6(e), and our duty to protect our vital national security interests.

As the courts have pointed out, "the scope of [grand jury] secrecy is necessarily broad. It encompasses not only the direct revelation of grand jury transcripts but also the disclosure of information which would reveal 'the identities of witnesses or jurors, the substance of testimony,

the strategy or direction of the investigation, the deliberations or questions of the jurors, and the like.'" *Fund for Constitutional Gov't v. Nat'l Archives & Records Serv.*, 656 F.2d 856, 859 (D.C. Cir. 1981), quoting *SEC v. Dresser Indus.*, 623 F.2d 1368, 1382 (D.C. Cir. 1980). The Department is, therefore, legally obligated to refrain from disclosing information that would reveal the strategy or direction of a grand jury investigation, or otherwise run afoul of the broad scope of the rule.

The grand jury secrecy rules serve very important governmental and societal interests. One important interest your question implicates is the the privacy of individuals who have participated in grand jury proceedings. These witnesses are not bound by Rule 6(e) - that these witnesses have not stepped forward and identified themselves, however, indicates that their privacy has been well served by our strict adherence to Rule 6(e).

And in terrorism investigations in particular, following the rules on grand jury secrecy also serves important national security interests. Terrorists and their supporters, who would seek to harm the United States, are interested in learning every detail of our efforts to detect, disrupt, and prosecute them. Obeying the rules on grand jury secrecy keeps valuable information out of their hands. There is also information that may be at the margins of Rule 6(e) protection that nonetheless may not be disclosed because of the harm that would inflict on our efforts to keep Americans safe. Often, in the grand jury context, these two rationales will overlap, which has been the case with respect to numerous information requests made in the past.

However, to the extent Congress is seeking aggregate numbers of material witness warrants, the Department believes that it can disclose this general information consistent with grand jury secrecy rules and with national security. Therefore, we have been working with the United States Attorneys' Offices to compile this data.

Of course, the numbers that follow are only approximate because the Department does not collect comprehensive data on the frequency with which U.S. Attorneys' Offices utilize the longstanding material witness authority under 18 U.S.C. § 3144. Nevertheless, in an effort to obtain information on the extent of use of this tool, we recently surveyed U.S. Attorneys' Offices and according to our informal survey, only in approximately 90 instances have material witness warrants been used in terrorism-related investigations since 9/11/2001. 28 districts reported that they have not used the material witness statute to detain anyone since 9/11/2001. In addition, our survey indicated that material witness warrants have been used approximately 230 times in investigations involving crimes such as drugs, guns and violent crimes since 9/11/2001. Of course, as the Committee has known for years, material witness warrants continue to be used regularly in alien smuggling cases. Indeed, our survey indicated that approximately 9,600 of the approximately 10,000 material witness warrants that have been issued since 9/11/2001 have been in alien smuggling and immigration related investigations.

The frequency with which these material witnesses have testified before the Grand Jury is difficult to estimate. As with the use of material witness authority, the Department does not collect comprehensive data on this, and we cannot even venture approximate figures. There are many reasons why an individual detained as a material witness might not testify before a grand

jury. It might well be the case that a material witness might not have testified before the grand jury because he or she struck a deal with the prosecution to become an informant, or because the thrust of his or her testimony may have been conveyed by another grand jury witness. In alien smuggling cases, which represent the vast majority of investigations in which material witness warrants are used, the individuals generally are detained for deposition and then released and deported. Given that the enabling statute requires very close supervision by the courts of the issuance of material witness warrants and affords significant procedural protections to material witnesses, we are confident that this authority is being properly used. From the outset, a court must issue a material arrest warrant – this is not a tool that a prosecutor can simply use absent prior court authorization. By statute, a material witness is entitled to an attorney; in the event he or she cannot afford an attorney, one will be provided. By statute, the individual is also entitled to a hearing before a judge. And the Federal Rules of Criminal Procedure require prosecutors to file frequent reports to the judge, keeping that judge appraised of the status of those detained as material witnesses.

41) **Before we grant new powers to combat terrorism, we should make certain that the Justice Department is using the authority it already has to keep dangerous weapons out of the hands of terrorists.**

The Justice Department's Inspector General recently issued a report detailing "critical deficiencies" in how the Bureau of Alcohol, Tobacco, Firearms, and Explosives is carrying out the Safe Explosives Act, which Congress passed shortly after 9/11. According to the report, 38,000 individuals had applied for a permit to use explosives. But the ATF failed to request an FBI background report on 9 percent of them - about 3,400 people.

Even when a background check was requested, the ATF failed to complete the clearance process 31 percent of the time. As a result, thousands of people remained in a "pending" status that allowed them to continue to use explosives for an average of 299 days.

Perhaps most troubling, in more than half of the cases (655 of 1,157) where the FBI background check had discovered criminal records or other red flags, the ATF failed to take action. The IG found one person who had four felony convictions who was allowed access to explosives.

Attorney General Gonzales, have you reviewed the Inspector General's report? And if so, are you disturbed by what it found?

ANSWER: While not related to the USA PATRIOT Act, the Attorney General is aware of the Inspector General's report on the implementation of the Safe Explosives Act (SEA). The Bureau of Alcohol, Tobacco, Firearms and Explosives provided a detailed response to the report which expressed appreciation for the recommendations provided by the Office of the Inspector General. In addition to noting some deficiencies, the Inspector General also positively acknowledged the accomplishments of ATF and its swift, efficient implementation of such

sweeping legislation. Some of the statistical findings in the OIG report were due to data entry errors, discrepancies in record keeping, and lack of available resources to resolve outstanding background checks. However, as a result of the report and other procedural improvements, ATF has taken steps to improve its enforcement of the SEA. For instance, ATF has increased staff at the Federal Explosives Licensing Center, made more training opportunities available to staff involved in conducting background checks, investigated and resolved the "pending individual" cases identified by the OIG report, and instituted new procedures for expeditiously resolving criminal histories that do not have definitive dispositions. Additionally, ATF has improved the data entry process to ensure that all appropriate databases are checked for each applicant and the FBI and ATF records reflecting these checks are comparable.

42) What are your plans to improve enforcement of the Safe Explosives Act?

ANSWER: The Bureau of Alcohol, Tobacco, Firearms and Explosives has been working diligently to enforce the Federal explosives laws, including the provisions added to Title 18 by the SEA. For instance, one new provision requires inspection of all explosives licensees and permits every three years. To satisfy this aspect of the SEA, ATF has increased its inspector workforce and has plans to offer additional training opportunities to inspectors related to explosives issues. ATF also enhanced its outreach efforts with the industry through seminars and partnerships to increase awareness of legal requirements and public safety issues. ATF further discussed its actions in this regard in the response to the Inspector General.

43) Last month, a GAO report found that 53 individuals on the FBI's terrorism watch list were allowed to purchase guns. These are people the government is tracking because they are suspected terrorists, and yet we're allowing them to buy guns right under our noses. Director Mueller testified before the House Appropriations Committee and he said that "We ought to look what can be done to perhaps modify the law to limit [suspected terrorists'] access to a weapon."

Would you support legislation prohibiting individuals on the FBI's "Violent Gang and Terrorist Organization File" from obtaining weapons?

ANSWER: While not related to the USA PATRIOT Act, the Attorney General has established a Department working group led by the Office of Legal Policy to review the question of whether additional legal authority should be sought with respect to the possession by or transfer of firearms to persons on the terrorist watch lists. We understand the working group has submitted its initial report, which the Attorney General is currently reviewing.

44) Please explain and provide the criteria used for determining when an individual will be added to the Violent Gang and Terrorist Organization File. What percentage of individuals included in the file have been added to the list as a result of an arrest, conviction or personal acknowledgment of involvement in gang or terrorist-related activity? Is there a process for an individual to have his or her name removed from the file? If so, please

explain.

ANSWER: While not related to the USA PATRIOT Act, the Violent Gang and Terrorist Organization File (VGTOF) is the file in the FBI's National Crime Information Center (NCIC) database with records on known or suspected members of violent gangs or terrorist organizations. The VGTOF is checked each time a federal, state, or local law enforcement agency runs a person's name against the NCIC and serves as a mechanism to share information with law enforcement about persons on the terrorist watchlist. Each terrorist record has a handling code that advises the querying agency of what steps to take when there is a hit on a suspected terrorist record.

The criteria for inclusion in VGTOF vary depending on whether the individual is suspected of involvement with violent gangs or terrorist organizations. In order to be listed in VGTOF, the full name and either the complete date of birth or passport number of the individual must be known. The records of terrorists in VGTOF are populated by individuals listed in the Terrorist Screening Database (TSDB), the combined Federal terrorist watchlist maintained by the Terrorist Screening Center (TSC). The TSDB consolidated the legacy watchlists, including the State Department's TIPOFF system, Custom and Border Patrol's TECS/IBIS, TSA's No-Fly/Selectee list, and the FBI's original VGTOF.

In accordance with HSPD-6, individuals are included in the TSDB as terrorists if they are "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." TSC receives new nominations for placement on the TSDB of international terrorism suspects from the National Counterterrorism Center (NCTC). TSC generally places everything sent by the NCTC into the TSDB unless TSC believes there is an insufficient corroboration of a terrorist nexus.

Individuals are included in VGTOF because of their suspected involvement with violent gangs if they meet any two of the following criteria: 1) the individual has been identified by an individual of proven reliability as a group member; 2) the individual has been identified by an individual of unknown reliability as a group member and that information has been corroborated in significant respects; 3) the individual has been observed by members of the entering agency to frequent a known group's area, associate with known group members, and/or affect the group's style of dress, tattoos, hand signals, or symbols; 4) the individual has been arrested on more than one occasion with known group members for offenses consistent with group activity; or 5) the individual has admitted membership in the identified group at any time other than arrest or incarceration. The group also must be an ongoing organization, association, or group of three or more persons and the group must have a common interest and/or activity characterized by the commission of or involvement in a pattern of criminal activity or delinquent conduct.

The vast majority of records contained in VGTOF are related to terrorism. The number of persons covered by records, however, is less than the total number of records, because there can be more than one record entry concerning the same individual. Approximately 97 percent of the records in VGTOF are terrorism-related and approximately 3 percent of the records are gang-related.

A terrorist subject remains in VGTOF until the case is closed or there is no longer a reason for the subject to remain on a watchlist. TSC is currently reviewing all TSDB records for Quality Assurance purposes, including a determination that there is a terrorist nexus for each TSDB entry. Individuals generally will not know if they are listed in VGTOF because they are considered to be terrorists. If the name of a specific individual is brought to the attention of TSC, however, TSC will conduct a review to determine whether the name still belongs in the TSDB and VGTOF. The names of violent gang members listed in VGTOF are purged every five years unless the originating agency takes steps to retain the individual in the file.

45) **Attorney General Gonzales, in your Senate testimony you said that the Administration's policy is that "we don't engage in torture, we don't condone torture, and we're not going to render people to countries where we think it's more likely than not that they're going to be tortured." That standard seems to be lower than the International Convention Against Torture, which prohibits the rendition of an individual "where there are substantial grounds for believing that he would be in danger of being subjected to torture."**

Is the Administration's policy not to render prisoners only if it is "more likely than not" they will be tortured? And if so, what is the standard for determining whether it's more likely than not that a person will be tortured? For example, what if it is determined that there is a 49% chance that they will be tortured? Or is the Administration adhering to the "substantial grounds" standard of the Geneva Convention?

ANSWER: The response to this question will be provided separately.